Privacy Impact Assessment

Version 1.3 / December 17, 1996

Office of Privacy Advocate
Internal Revenue Service
1111 Constitution Ave., NW
Washington, DC 20224

TABLE OF CONTENTS

Section I
Introduction and Overview . . . . . page 1

Section II
Privacy Impact Assessment . . . . . page 2

Section III
Completing a Privacy Impact Assessment . . . . . page 3

Section IV
Privacy Issues in Information Systems . . . . . page 4

Section V
Privacy Questions . . . . . page 9

Appendix A
Declaration of Privacy Principles . . . . . page 11

Appendix B
Policy Statement on Taxpayer Privacy Rights . . . . . page 13

SECTION 1

Introduction and Overview

Introduction

The Internal Revenue Service recognizes the importance of protecting the privacy of taxpayers and employees, especially as it modernizes its tax and employee systems. Privacy issues must be addressed when systems are being developed, and privacy protections must be integrated into the development life cycle of these automated systems. The vehicle for addressing privacy issues in a system under development is the Privacy Impact Assessment (PIA). The PIA process also provides a means to assure compliance with applicable laws and regulations governing taxpayer and employee privacy.

Purpose

The purpose of this document is to:

- Establish the requirements for addressing privacy during the systems development process;
- Describe the steps required to complete a PIA on a project;
- Define the privacy issues a project must address when completing a PIA.

Background

The Internal Revenue Service is responsible for ensuring the privacy, confidentiality, integrity, and availability of taxpayer and employee information. The IRS recognizes that privacy protection is both a personal and fundamental right of all taxpayers and employees. Among the most basic of taxpayers' and employees' rights is an expectation that the Service will protect the confidentiality of personal, financial, and employment information. Taxpayers and employees also have the right to expect that the Service will collect, maintain, use, and disseminate identifiable personal information and data only as authorized by law and as necessary to carry out agency responsibilities. Taxpayer and employee information is protected by the following:

- Privacy Act of 1974, as Amended (5 USC 552a) which affords individuals the right to privacy in records that are maintained and used by Federal agencies. Note that 5 USC 552a includes the Computer Matching and Privacy Act of 1988 (Public Law 100-503);
- Computer Security Act of 1987 (Public Law 100-235) which establishes minimum security practices for Federal computer systems;
- Internal Revenue Code Section 6103, Confidentiality and Disclosure of Return and Return Information;

■ OMB Circular A-130, Management of Federal Information Resources, which provides instructions to Federal agencies on how to comply with the fair information practices and security requirements for operating automated information systems;

■ Freedom of Information Act, as Amended (5 USC 552) which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.

Office of the Privacy Advocate

The Office of the Privacy Advocate is the IRS organization responsible for overseeing taxpayer and employee privacy. The Office was established in January 1993 under the Chief Information Officer. The mission of the Office of the Privacy Advocate is to formulate, develop, implement, and promote effective taxpayer and employee privacy protection strategies and programs. These strategies and programs will enhance the efforts of the Service to earn the highest degree of public confidence in its integrity, efficiency, and fairness. The Office of the Privacy Advocate developed the Privacy Principles, which were disseminated by the Commissioner in May 1994. Policy Statement P-1-1, "Taxpayer Privacy Rights" was signed by the Commissioner in October 1994. The Privacy Principles are in Appendix A and the Policy Statement is in Appendix B of this document.

SECTION II

Privacy Impact Assessment

Privacy and Systems Development

Rapid advancements in computer technology make it possible to store and retrieve vast amounts of data of all kinds quickly and efficiently. These advancements have raised concerns about the impact of large computerized information systems on the privacy of data subjects. Public concerns about highly integrated information systems operated by the government make it imperative to commit to a positive and aggressive approach to protecting individual privacy. The Office of the Privacy

Advocate has instituted the Privacy Impact Assessment in order to ensure that the systems the IRS develops protect individuals' privacy. The PIA incorporates privacy into the development life cycle so that all system development initiatives can appropriately consider privacy issues from the earliest stages of design.

What is a Privacy Impact Assessment?

The Privacy Impact Assessment is a process used to evaluate privacy in information systems. The process is designed to guide system owners and developers in assessing privacy through the early stages of development. The process consists of privacy training, gathering data from a project on privacy issues, identifying and resolving the privacy risks, and approval by the Privacy Advocate. The PIA process is described in detail in Section III, Completing a Privacy Impact Assessment.

When is a PIA Done?

The PIA is to be initiated in the early stages of the development of a system and completed as part of the required System Life Cycle (SLC) reviews. Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and system design. This applies to all of the development methodologies and system life cycles used in the Service.

Who completes the PIA?

Both the system owner and system developers must work together to complete the PIA. System owners must address what data is to be used, how the data is to be used, and who will use the data. The system developers must address whether the implementation of the owner's requirements presents any threats to privacy.

What Systems Have to Complete a PIA

New systems, systems under development, or systems undergoing major modifications are required to complete a PIA. The Privacy Advocate does reserve the right to request that a PIA be completed on any system that may have privacy risks. More specifically:

- New systems and systems under development or undergoing major modifications are required to complete a PIA.
- Legacy systems, as they exist today, do not have to complete a PIA. However, if the automation or upgrading of these systems puts the data at risk, a PIA may be requested by the Privacy Advocate.
- Currently operational systems are not required to complete a PIA. However, if privacy is a concern for a system the Privacy Advocate can request that a PIA be completed. If a potential problem is identified concerning a currently operational system, the Service will use best, or all reasonable, efforts to remedy the problem.

SECTION III

Completing a Privacy Impact Assessment

The PIA

This section describes the steps that are required to complete a PIA. These steps are summarized in Table 1, Outline of Steps for Completing a PIA.

Training

Training on the PIA will be available, upon request, from the Office of the Privacy Advocate. The training describes the PIA process and provides detail about the privacy issues and privacy questions to be answered to complete the PIA. The intended audience is the personnel responsible for writing the PIA document. PIA training is available to government and contractor personnel.

The PIA Document

Preparing the PIA document requires the system owner and developer to answer the privacy questions in Section V. A brief explanation should be written for each question. Issues that do not apply to a system should be noted as "Not Applicable". During the development of the PIA document, the Office of the Privacy Advocate will be available to answer questions related to the PIA process and other concerns that may arise with respect to privacy.

Review of the PIA Document

The completed PIA document is to be submitted to the Office of the Privacy Advocate for review. The purpose of the review is to identify privacy risks in the system. The Office of the Privacy Advocate will work with the system owner and system developer to develop design requirements to resolve the identified risks. If there are risks in a system that cannot be resolved with the Privacy Advocate, the risks will be presented to the Chief Information Officer (CIO) for resolution.

Approval of the PIA

The SLC review process will be used to validate the incorporation of the design requirements to resolve the privacy risks. Formal approval will be issued in accordance with the SLC.

Table 1

Outline of Steps for Completing a PIA

Step	Who	Procedure
1	System Owner, and Developer	Request and complete Privacy Impact Assessment (PIA) Training.
2	System Owner, and Developer	Answer the questions in Section V, Privacy Questions.
3	System Owner, and Developer	Submit the PIA document to the Privacy Advocate.
4	Office of the Privacy Advocate (PA)	Review the PIA document to identify privacy risks from the information provided. The Privacy Advocate will get clarification from the owner and developer as needed.
5	System Owner, Developer, PA, and CIO	The System Owner, Developer, and the Privacy Advocate should reach agreement on design requirements to resolve all identified risks. If an agreement cannot be reached, then issues will be raised to the CIO for resolution.
6	System Owner, and Developer	The System Owner and Developer will incorporate the agreed upon design requirements and resolve the identified risks.
7	System Owner, Developer, and PA	Participate in the SLC required reviews to ensure satisfactory resolution of identified privacy risks and obtain formal approval.

SECTION IV

Privacy Issues in Information Systems

Privacy Act of 1974 5 U.S.C. 552a As Amended

The Privacy Act of 1974 5 U.S.C. 552a As Amended requires Federal Agencies to protect personally identifiable information. It states specifically:

"each agency that maintains a system of records shall –"

■ "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;"

■ "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;"

■ "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;"

■ "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

Definitions

Accuracy - within sufficient tolerance for error to assure the quality of the record in terms of its use in making a determination.

Completeness - all elements necessary for making a determination are present before such determination is made.

Determination - any decision affecting an individual which, in whole or in part, is based on information contained in the record and which is made by any person or agency.

Necessary - a threshold of need for an element of information greater than mere relevance and utility.

Record - any item, collection or grouping of information about an individual and identifiable to that individual that is maintained by an agency.

Relevance - limitation to only those elements of information which clearly bear on the determination(s) for which the records are intended.

Routine Use - with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

System of Records - a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Timeliness - sufficiently current to ensure that any determination based on the record will be accurate and fair.

Information and Privacy

To fulfill the commitment of the IRS to protect taxpayer data several issues must be addressed with respect to privacy.

- The use of information must be controlled.
- Information may be used only for a necessary and lawful purpose.
- Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them.
- Information collected for a particular purpose should not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
- Any information used must be sufficiently accurate, relevant, timely, and complete to assure fair treatment of the individual.

Given the availability of vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the IRS, to share that information. With the potential expanded uses of data in automated systems it is important to remember that information can only be used for the purpose for which it was collected unless other uses are specifically authorized or mandated by law. If the data is to be used for other purposes, then the public must be provided notice of those other uses.

These procedures do not in themselves create any legal rights, but are intended to express the full and sincere commitment of the Service to the laws which protect taxpayer and employee privacy rights and which provide redress for violations of those rights.

Data in the System

The sources of the information in the system are an important privacy consideration if the data is gathered from other than IRS records. Information collected from non-IRS sources should be verified, to the extent practicable, for accuracy, that the information is current, and the information is complete. This is especially important if the information will be used to make determinations about individuals.

Access to the Data

Who has access to the data in a system must be defined and documented. Users of the data can be individuals, other systems, and other agencies. Individuals who have access to the data can be system users, system administrators, system owners, managers, and developers. When individuals are granted access to a system, their access should be limited, where possible, to only that data needed to perform their assigned duties. If individuals are granted access to all of the data in a system, procedures need to be in place to deter and detect browsing and unauthorized access. Other systems are any programs or projects that interface with the system and have access to the data. Other agencies can be International, Federal, State, or Local entities that have access to IRS data.

Attributes of the Data

When requirements for the data to be used in the system are being determined, those requirements must include the privacy attributes of the data. The privacy attributes are derived from the legal requirements imposed by the Privacy Act of 1974. First, the data must be relevant and necessary to accomplish the purpose of the system. Second, the data must be complete, accurate, and timely. It is important to ensure the data has these privacy attributes in order to assure fairness to the individual in making decisions based on the data.

Maintenance of Administrative Controls

Automation of systems can lead to the consolidation of processes, data, and the controls in place to protect the data. When administrative controls are consolidated, they should be evaluated so that all necessary controls remain in place to the degree necessary to continue to control access to and use of the data.

Data retention procedures should be documented. Data retention procedures require review to ensure they meet statutory and/or Internal Revenue Manual (IRM) requirements. Precise rules must be established for the length of time information is kept and for assuring that it is properly eliminated at the end of that time.

The intended and potential monitoring capabilities of a system must be defined and safeguards must be installed to ensure the privacy of taxpayers and prevent unnecessary intrusion. The use of monitoring capabilities should be limited, at a minimum, to some judicially ascertainable standard of reasonableness in light of the statutory mission of the IRS and other authorized governmental users of the system.

SECTION V

Privacy Questions

Data in the System

1. Generally describe the information to be used in the system in each of the following categories: Taxpayer, Employee, and Other.

2. What are the sources of the information in the system?

a. What IRS files and databases are used?

b. What Federal Agencies are providing data for use in the system?

c. What State and Local Agencies are providing data for use in the system?

d. From what other third party sources will data be collected?

e. What information will be collected from the taxpayer/employee?

3. a. How will data collected from sources other than IRS records and the taxpayer be verified for accuracy?

b. How will data be checked for completeness?

c. Is the data current? How do you know?

4. Are the data elements described in detail and documented? If yes, what is the name of the document?

Access to the Data

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?

5. a. Do other systems share data or have access to data in this system? If yes, explain.

b. Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?

6. a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

b. How will the data be used by the agency?

c. Who is responsible for assuring proper use of the data?

d. How will the system ensure that agencies only get the information they are entitled to under IRC 6103?

Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

2. a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

b. Will the new data be placed in the individual's record (taxpayer or employee)?

c. Can the system make determinations about taxpayers or employees that would not be possible without the new data?

d. How will the new data be verified for relevance and accuracy?

3. a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.

What are the potential effects on the due process rights of taxpayers and employees of:

a. consolidation and linkage of files and systems;

b. derivation of data;

c. accelerated information processing and decision making;

d. use of new technologies.

How are the effects to be mitigated?

Maintenance of Administrative Controls

1. a. Explain how the system and its use will ensure equitable treatment of taxpayers and employees.

b. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

c. Explain any possibility of disparate treatment of individuals or groups.

2. a. What are the retention periods of data in this system?

b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

3. a. Is the system using technologies in ways that the IRS has not previously employed (e.g. Caller-ID)?

b. How does the use of this technology affect taxpayer/employee privacy?

4. a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

c. What controls will be used to prevent unauthorized monitoring?

5. a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.

b. If the system is being modified, will the SOR require amendment or revision? Explain.

APPENDIX A

Declaration of Privacy Principles

The privacy principles set forth in this declaration are based on the ethical and legal obligations of the Internal Revenue Service to the taxpaying public and are the responsibility of all IRS employees to recognize and treat their office as a public trust.

The obligation to protect taxpayer privacy and to safeguard the information taxpayers entrust to us is a fundamental part of the Service's mission to administer the tax law fairly and efficiently. Taxpayers have the right to expect that the information they provide will be safeguarded and used only in accordance with law. In recognition of these obligations, policies and procedures must clearly state who should have access to what information and for what purposes. In addition, appropriate limitations must be placed on the collection, use, and dissemination of taxpayer's personal and financial information, and sufficient technological and administrative measures must be implemented to ensure the security of IRS data systems, processes, and facilities.

All IRS employees are required to exhibit individual performance that reflects a commitment to dealing with every taxpayer fairly and honestly and to respect the taxpayer's right to feel secure that their personal information is protected. To promote and maintain taxpayers' confidence in the privacy, confidentiality and security protections provided by the IRS, the Service will be guided by the following Privacy Principles:

Principle 1

Protecting taxpayer privacy and safeguarding confidential taxpayer information is a public trust.

Principle 2

No information will be collected or used with respect to taxpayers that is not necessary and relevant for tax administration and other legally mandated or authorized purposes.

Principle 3

Information will be collected, to the greatest extent practicable, directly from the taxpayer to whom it relates.

Principle 4

Information about taxpayers collected from third parties will be verified to the greatest extent practicable with the taxpayers themselves before action is taken against them.

Principle 5

Personally identifiable taxpayer information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.

Principle 6

Personally identifiable taxpayer information will be disposed of at the end of the retention period required by law or regulation.

Principle 7

Taxpayer information will be kept confidential and will not be discussed with, nor disclosed to, any person within or outside the IRS other than as authorized by law and in the performance of official duties.

Principle 8

Browsing, or any unauthorized access of taxpayer information by any IRS employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.

Principle 9

Requirements governing the accuracy, reliability, completeness, and timeliness of taxpayer information will be such as to ensure fair treatment of all taxpayers.

Principle 10

The privacy rights of taxpayers will be respected at all times and every taxpayer will be treated honestly, fairly, and respectfully.

The Declaration does not, in itself, create any legal rights for taxpayers, but it is intended to express the full and sincere commitment of the Service and its employees to the laws which protect taxpayer privacy rights and which provide redress for violations of those rights.

APPENDIX B

Policy Statement on Taxpayer Privacy Rights

The IRS is fully committed to protecting the privacy rights of all taxpayers. Many of these rights are stated in law. However, the Service recognizes that compliance with legal requirements alone is not enough. The Service also recognizes its social responsibility which is implicit in the ethical relationship between the Service and the taxpayer. The components of this ethical relationship are honesty, integrity, fairness, and respect.

Among the most basic of a taxpayer's privacy rights is an expectation that the Service will keep personal and financial information confidential. Taxpayer's also have the right to expect that the Service will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities.

The Service will safeguard the integrity and availability of taxpayers' personal and financial data and maintain fair information and record keeping practices to ensure equitable treatment of all taxpayers. IRS employees will perform their duties in a manner that will recognize and enhance individuals' rights of privacy and will ensure that their activities are consistent with law, regulations, and good administrative practice. In our record keeping practices, the Service will respect the individual's exercise of his/her First Amendment rights in accordance with law.

As an advocate for privacy rights, the Service takes very seriously its social responsibility to taxpayers to limit and control information usage as well as to protect public and official access. In light of this responsibility, the Service is equally concerned with the ethical treatment of taxpayers as well as their legal and administrative rights.

Department of the Treasury
Internal Revenue Service

w w w . i r s . g o v

Publication 3656 (8-2000)
Catalog Number 30605X